IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, *et al.*,

Plaintiffs,

v.

BRAD RAFFENSPERGER, *et al.*,

Defendants.

CIVIL ACTION NO.
1:17-CV-2989-AT

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF PLAINTIFFS' POSITION AT TRIAL

Marc Rotenberg
EPIC President and Executive Director

Alan Butler (pro hac vice)
EPIC Senior Counsel

Caitriona Fitzgerald
EPIC Policy Director

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140
Counsel for the Electronic Privacy Information Center

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF THE AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] EPIC frequently participates as *amicus curiae* in federal and state court cases that implicate emerging privacy issues, including voter privacy. *See, e.g.*, Brief of *Amici Curiae* EPIC et. al, *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008) (opposing voter photo-ID requirements as infringing on citizens' right to cast a secret ballot); Brief of *Amici Curiae* EPIC et al., *Doe v. Reed*, 561 U.S. 186 (2010) (arguing that the First Amendment protects the right to anonymity in referenda signatures); *Brief of Amici Curiae* EPIC et al., *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002) (supporting First Amendment Right to anonymous door-to-door speech).

EPIC seeks to ensure the integrity of voting equipment and also to preserve the secret ballot, the well-established right of individuals to remain anonymous while voting. EPIC's advisory board includes distinguished

[1] EPIC IPIOP Law Clerk Sonali Seth assisted in the preparation of this brief.

experts in law, technology, and public policy, including several who have pioneered techniques for election security and privacy protection.[2]

---

[2] *See, e.g.*, David Chaum, *Achieving Electronic Privacy*, Scientific American 96-101 (Aug. 1992) ("Over the past eight years, my colleagues and I . . . have developed a new approach, based on fundamental theoretical and practical advances in cryptography, that . . . avoid the possibility of fraud while maintaining the privacy of those who use them [to complete transactions]."); Gary T. Marx, *What's in a Concept? Some Reflections on the Complications and Complexities of Personal Information and Anonymity*, 3 U. Ottawa L. & Tech. J. 1, 19 (2006) ("We seek privacy and often anonymity, but we also know that secrecy can hide dastardly deeds and that visibility can bring accountability. But too much visibility may inhibit experimentation, creativity and risk taking."); Stefan Brands, *Non-Intrusive Cross-Domain Digital Identity Management*, Presented at Proceedings of the 3rd Annual PKI R&D Workshop (Apr. 2004), *available at* http://www.idtrail.org/files/cross_domain_identity.pdf ("The distinction is critical; many authentication systems provide security while preserving anonymity by allowing for the separation of attributes and identification."); Alessandro Acquisti, et al., *On the Economics of Anonymity*, Financial Cryptography, 84-102 (2003) ("Individuals and organizations need anonymity on the Internet. People want to surf the Web, purchase online, and send email without exposing to others their identities, interests, and activities."); Latanya Sweeney, *Anonymity: A Model for Protecting Privacy*, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 557-70 (2002) ("In many cases the survival of the database itself depends on the data holder's ability to produce anonymous data because not releasing such information at all may diminish the need for the data, while on the other hand, failing to provide proper protection within a release may create circumstances that harm the public or others."); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000) ("The recognition that anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association—decisions that otherwise might be chilled by unpopularity or simple difference—is part of our constitutional tradition."); Anita Allen, *Coercing Privacy*, 40 Wm. & Mary L. Rev. 723, 756 (1999) ("There is both empirical evidence and normative philosophical argument supporting the proposition that paradigmatic forms of privacy (e.g., seclusion, solitude, confidentiality, secrecy, anonymity) are vital to well-being. It is

EPIC's brief is joined by the following legal scholars and technical experts:

Legal Scholars and Technical Experts

Rod Beckstrom
Founder and CEO of BECKSTROM

James Bamford
Author and Journalist

Colin Bennett
Professor, University of Victoria

David Chaum
CEO/Founder, Elixxir

Danielle Keats Citron
Morton & Sophia Macht Professor of Law, Univ. of Maryland Carey School of Law

Addison Fischer
Founder and Chairman, Fischer International Corp.

David Flaherty
Former Information and Privacy Commissioner for British Columbia

Rush Holt
Former Member of Congress

Jerry Kang
Korea Times—Hankook Ilbo Chair in Korean Am. Studies and Law, UCLA

---

not simply that people need opportunities for privacy; the point is that their well-being, and the well-being of the liberal way of life, requires that they in fact experience privacy."); Jerry Kang, *Cyberspace Privacy*, 50 Stan. L. Rev. 1193, 1209 (1998) ("[W]e must recognize that anonymity comes in shades. Although no specific individual is identified facially, the individual may be identifiable in context or with additional research. . . .").

Len Kennedy
Senior Advisor, Neustar, Inc.

Lorraine G. Kisselburgh
Visiting Lecturer and Faculty Fellow, Discovery Park Center for Entrepreneurship and Center for Research in Information Security, Purdue University

Chris Larsen
Executive Chairman, Ripple Inc.

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Roger McNamee
Co-Founder, Elevation Partners

Mary Minow
Librarylaw.com

Pablo Garcia Molina
Adjunct Professor, Georgetown University

Peter G. Neumann
Chief Scientist, SRI International Computer Science Lab

Helen Nissenbaum
Professor, Cornell Tech Information Science

Stephanie Perrin
President, Digital Discretion, Inc.

Bilyana Petkova
Assistant Professor, Department of International and European Law, Maastricht University

Ray Ozzie
Founder, Talko

Deborah C. Peel, MD
Founder and Chair, Patient Privacy Rights

Ron L. Rivest
Institute Professor of Electrical Engineering and Computer Science, MIT

Bruce Schneier
Fellow and Lecturer, Harvard Kennedy School

Barbara Simons
IBM Research (retired)

Sherry Turkle
Abby Rockefeller Mauzé Professor of the Social Studies of Science and Technology, Massachusetts Institute of Technology
Founding Director, MIT Initiative on Technology and Self

Edward G. Viltz
President and Chairman, Internet Collaboration Coalition

Ari Ezra Waldman
Professor of Law, New York Law School

Jim Waldo
Gordon McKay Professor of the Practice of Computer Science and Chief Technology Officer, John A. Paulson School of Engineering and Applied Sciences at Harvard University

Christopher Wolf
Board Chair, Future of Privacy Forum

Shoshana Zuboff
Charles Edward Wilson Professor of Business Administration, Emerita Harvard Business School

(Affiliations are for identification only)

ARGUMENT

Since almost the moment direct recording electronic (DRE) voting machines were introduced, computer scientists and cybersecurity experts have warned that these machines are unreliable, insecure, and unverifiable. This has led many states to replace DRE machines, but Georgia has not, leaving Georgia's elections subject to attack. Beyond the security issues, Georgia's DRE machines also compromise the secret ballot. The secret ballot is the cornerstone of our democracy, allowing voters the ability to exercise their right to vote without intimidation or retaliation. The use of DREs threaten our democracy and should be removed from use in our elections.

I. DRE voting systems are subject to manipulation, attack, and fraud.

A. Security experts have identified many flaws with DRE voting systems.

Direct recording electronic (DRE) voting machines are subject to manipulation, attack, and fraud. In an extensive report concerning the integrity of voting systems and the risks associated with digital technology, the National Academies of Sciences recently determined:

> [A]ll digital information—such as ballot definitions, voter choice records, vote tallies, or voter registration lists— is subject to malicious alteration; there is no technical mechanism currently available that can ensure that a computer application— such as one used to record or count votes— will produce accurate results;

> testing alone cannot ensure that systems have not been compromised; and any computer system used for elections— such as a voting machine or e-pollbook— can be rendered inoperable.

National Academies of Sciences, Engineering, and Medicine, et al. *Securing the Vote: Protecting American Democracy* 42, 80 (National Academies Press, 2018) ("National Academies Report.")

But this is not news. For many years, computer scientists and cybersecurity experts have warned election officials that paperless balloting systems, and in particular DRE machines, are unreliable, insecure, and unverifiable. *See* Eric A. Fischer, Cong. Research Serv., RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues* (2003) ("there appears to be an emerging consensus that in general, current DREs do not adhere sufficiently to currently accepted security principles for computer systems"). The necessary criteria for electronic voting security have long been known – and DREs repeatedly fail to meet them. Peter G. Neumann, National Computer Security Conference, *Security Criteria for Electronic Voting* (Sept. 20-23, 1993) (establishing the importance of reliability, accountability, and disclosability); U.S. Election Assistance Commission, Proposed Voluntary Voting System Guidelines 2.0 Principles

and Guidelines, 84 FR 6775 (Feb. 28, 2019) ["EAC Guidelines"] (setting ballot secrecy, voter privacy, and auditability as fundamental principles).[3]

States adopted electronic voting machines with federal funding provided by the 2002 Help America Vote Act, a response to election security controversies in the 2000 presidential election. The Caltech/MIT Voting Technology Project, *Voting: What Has Changed, What Hasn't, & What Needs Improvement* (Jan. 2013). Yet, almost immediately, researchers began to uncover serious vulnerabilities in DREs. After the source code for a DRE voting machine was accidentally posted online, researchers found that the software demonstrates significant flaws. Tadayoshi Kohno, et al., *Analysis of an Electronic Voting System*, 2004 IEEE Symposium on Security and Privacy 27 (2004). Vulnerabilities include network attacks, unauthorized privilege escalation, incorrect use of cryptography, and poor software development processes. *Id.* For example, all systems studied in the 2004 IEEE report used the same encryption key, rendering the encryption virtually useless. *Id*. As a result, "even the most serious of our outsider attacks could have been discovered and executed without access to the source code[, and] the insider threat is also quite considerable." *Id*. A "top-to-bottom" review of DRE voting

[3] https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf.

machines commissioned by California Secretary of State Debra Bowen in 2007 found the systems were susceptible to viruses and malicious software ("malware"). Joseph A. Calandrino, et al., *Source Code Review of the Diebold Voting System* 10, Univ. of Cal. (July 20, 2007).[4] The DRE machines reviewed in the California study were newer – and therefore presumably more secure – than the DRE machines used in Georgia. Following the California review, Secretary Bowen temporarily decertified California's Diebold DRE machines pending security changes, finding that the machines were "inadequate to ensure accuracy and integrity of the election results." Calif. Sec. of State, *Withdrawal Of Approval* 2 (Dec. 31, 2009 rev.).[5]

Installing viruses or malware on DRE machines is relatively easy. Researchers Ariel Feldman, Alex Halderman, and Edward Felten studied the AccuVote TS DRE machine (the same machines still used in Georgia today) in 2006 and found that "anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes *as little as one minute*." Ariel J. Feldman, J. Alex Halderman, & Edward W. Felten, *Security*

[4] https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf.
[5] http://votingsystems.cdn.sos.ca.gov/vendors/premier/premier-11824-revision-1209.pdf.

Analysis of the Diebold AccuVote-TS Voting Machine, USENIX/ACCURATE Electronic Voting Technology Workshop (2007) (emphasis added).

These attacks could take multiple forms. A computer virus could subtly steal votes from one candidate and assign them to another, evading detection by keeping the overall vote totals intact. *Id.* An attacker could install malware that would cause votes to be tabulated incorrectly or stop the machine from accepting votes. Calandrino, *supra*, at *i.* Even if an attacker had access to just one memory card, Diebold DREs are susceptible to computer viruses that could spread between DREs or between DREs and the election management system, enabling "large-scale election fraud." *Id.* An attacker could also institute a massive denial of service by shutting down voting machines, destroying records, or slowing down voting in order to affect outcomes and sow chaos into the voting process. *Id.* at 14. Worse still, Professor J. Alex Halderman demonstrated last year that Diebold DRE machines can be hacked remotely, which would allow foreign adversaries to stage an attack on elections without any physical access to voting machines. J. Alex Halderman, Op-Ed., *I Hacked an Election. So Can the Russians*, N.Y.

Times (Apr. 5, 2018).[6] Voter disenfranchisement is also a real possibility. Professor Latanya Sweeney has explained that on Election Day an attacker could change a voter's address in state voter registration databases, forcing the voter to fill out a provisional ballot that will later be deemed ineligible. *Election Sec.: Voting Tech. Vulnerabilities: Hearing Before the Subcomm. on Investigations & Oversight and Subcomm. on Research & Tech. of the H. Comm. on Sci., Tech., and Space*, 116th Cong. (2019) (statement of Latanya Sweeney, Professor at Harvard University).

While DREs provide multiple opportunities for hackers to install viruses or malware, errors are notoriously difficult to detect. "DRE software is moderately complex, and it is generally accepted that the more complex a piece of software is, the more difficult it can be to detect unauthorized modifications." Cong. Research Serv., *supra* at 6. DRE technology is entirely capsulated inside a single computer, so it is "software-dependent;" an undetected change or error in the system's software can cause an undetectable change or error in the election outcome. Ronald L. Rivest & John P. Wack, *On the Notion of Software Independence in Voting Systems*,

[6] https://www.nytimes.com/2018/04/05/opinion/election-voting-machine-hacking-russians.html.

366 Philosophical Transactions: Mathematical, Physical and Eng'g Sciences 3759 (Oct. 28, 2008); *see also* Sujata Garera et al., *An Independent Audit Framework for Software Dependent Voting Systems*, ACM Conference on Computer and Communications Security 257 (2007). The current draft of the Election Assistance Commission's Guidelines requires software independence. EAC Guidelines, *supra* at Principle 9. Although DRE touchscreen monitors might appear to be counting ballots, because an election official "can't watch the bits inside," the machine might be marking votes as errors or awarding them to other candidates. Ronnie Dugger, *How They Could Steal the Election This Time*, The Nation (July 29, 2004) (quoting Peter Neumann); As voting technology experts have explained, "[a] computer can easily display one set of votes on the screen for confirmation by the voter while recording entirely different votes in electronic memory, either because of a programming error or a malicious design." David L. Dill, Bruce Schneier & Barbara Simons, *Voting and Technology: Who Gets to Count Your Vote?*, 46 Communications of the ACM 29 (Aug. 2003). Security experts consider software-dependent voting systems "unacceptable" by security standards because an adversary can change an election outcome *without fear of detection*. Rivest, *supra*, at 3761.

The DRE market and the absence of effective regulations compound the problem. DRE vendors are not subject to any federal regulatory requirements. Nat'l Conference of State Legislatures, *Voting Systems, Standards, and Certification* (Aug. 6, 2018).[7] Code secrecy agreements prevent election officers from examining the software for DRE machines. Dill, Schneier & Simons, *supra* at 29. As a result, programmers cannot scrutinize the code to find cybersecurity weaknesses, evidence of tampering, or opportunities to improve the source code design. Andrew Massey, *But We Have to Protect Our Source: How Electronic Voting Companies' Proprietary Code Ruins Elections*, 27 Hastings Commc'ns & Entm't L. J. 233, 235–40 (Jan. 1, 2004).[8] "In practice, proprietary code-based DREs have proven to be error-ridden and prone to security weaknesses because the closed nature of the code has forced state agencies to protect manufacturers' intellectual property at the expense of a reliable voting system." *Id*. at 235. The use of proprietary source code in electronic voting machines undermines government transparency, regulatory accountability, and election security. To prevent interference and widespread distrust in election systems, it is

[7] http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx#Sets%20Standards.
[8] https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1605.

essential that states reduce their reliance on electronic systems. As the National Academies of Science has explained:

> [b]ecause there is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats, one must adopt methods that can assure the accuracy of the election outcome without relying on the hardware and software used to conduct the election.

National Academies Report at 91. The chairman of the House Intelligence Committee has expressed similar concerns about electronic voting systems. "The one thing we've been warning about for many, many years on the Intelligence committee is about the electronic voting systems," said Chairman Nunes. Julia Manchester, *House Intel Chair Calls For Ban On Electronic Voting Systems*, The Hill (July 26, 2018).[9]

The security weaknesses of electronic voting machines, and DREs in particular, have been obvious for many years. The National Academies Report makes clear what is widely known in the computer research community: DREs are unsafe for vote tabulation.

[9] https://thehill.com/hilltv/rising/398949-house-intel-chair-calls-for-ban-on-electronic-voting-systems.

B. Several states have removed DRE voting systems.

Fortunately, DRE voting systems are not the most common election system used in the United States. *The Verifier – Polling Place Equipment,* Verified Voting (Nov. 2018).[10] According to a study released this week by the Election Assistance Commission, in 2018 96.3 percent of states used optical or digital scanners to scan paper ballots in at least one jurisdiction. Election Assistance Comm'n, *Overview of Election Administration and Voting in 2018* 20 (Jun. 27, 2019).[11]

Many Secretaries of State heeded the warnings of computer scientists and led efforts to investigate security issues with DRE machines. In 2007, State Secretaries in Colorado, Kentucky, Ohio, and California conducted investigations into their states' voting systems. Jocelyn F. Benson, *State Secretaries of State: Guardians of the Democratic Process* 106 (2010). California's above-mentioned 2007 review resulted in the temporary decertification of Diebold DRE voting machines in use in the state until certain security conditions were met. Christopher Drew, *California Restricts Voting Machines*, N.Y. Times (Aug. 5, 2007).[12] Colorado Secretary of State

[10] https://www.verifiedvoting.org/verifier/.
[11] https://www.eac.gov/assets/1/6/2018_EAVS_Report.pdf.
[12] https://www.nytimes.com/2007/08/05/us/05vote.html.

Mike Coffman also decertified almost all the electronic voting machines in Colorado and until the vendors met strict testing requirements. Benson, *supra*; Press Release, Colorado Secretary of State, *Coffman Strengthens Testing Requirements For Electronic Voting Machines* (March 20, 2007).[13]

Ohio Secretary of State Jennifer Brunner's study of her state's electronic voting system predictably led to similar conclusions. Secretary Brunner's Evaluation and Validation of Election-Related Equipment, Standards and Testing ("EVEREST") initiative – which, like California, examined an even newer version of Diebold DRE machines than Georgia uses – found that the machines were extremely vulnerable to hacking, including one attack that only required 30 seconds and a ball point pen. Secretary of State Jennifer Brunner, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing* 141 (Dec. 2007).[14] Following the report, Secretary Brunner worked with the Ohio Legislature to eliminate Ohio's electronic voting machines. Benson, *supra*, at 108.

After a security assessment in 2017, Virginia decertified its DRE machines that were still in use and eliminated them completely from

[13]https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2007/PR20070320VotingMachines.html.
[14] https://security.cs.georgetown.edu/~msherr/papers/everest-ohio.pdf.

elections "in an effort to increase the security and integrity of Virginia's voting systems." Press Release, Virginia Department of Elections, *Virginia Decertifies Paperless Voting Equipment* (Sept. 8, 2017).[15] Last year, Kansas enacted a law prohibiting counties from purchasing new DREs and mandates that any electronic voting systems purchased in the future provide a paper record when the vote is cast and are capable of being audited. 2018 Kan. Sess. Laws 1238. Kentucky Secretary of State Alison Grimes called for the replacement of all paperless voting systems in her state in 2018. Bradford Queen, *Grimes Leads Board of Elections in Move to Require Voter-Verified Paper Trails in Kentucky*, Kentucky.gov (Feb., 27, 2018).[16]

Jurisdictions choosing to box up the DREs have many alternatives. The most commonly used election system, and current best practice from a security perspective, is optical scanning, in which voters mark paper ballots and voter responses are tabulated using computerized optical scanners, similar to scanners used for standardized tests. National Academies Report at 39.

[15] https://www.elections.virginia.gov/media/Media/ELECTNewsRelease-09-08-17.pdf.
[16] https://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&prId=156.

C. Hand-marked paper ballots, combined with mandatory post-election audits, are considered the best practice.

Georgia's DRE machines includes no physical or paper ballot, which prevents post-election audit trail. As a result, voters cannot verify that their votes are correctly recorded. David Chaum, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, 2 IEEE Comput. Soc'y 38 (2004).[17] Moreover, since the ballot itself is embedded in the same equipment that counts the ballot and Georgia does not use paper ballots, verification by ballot recount is impossible. According to the near-unanimous consensus of the computer science and election security communities, the absence of a paper trail exacerbates major cybersecurity risks and deteriorates public confidence in the integrity of elections. As the National Academies stated, "without a paper record, it is not possible to conduct a convincing audit of the results of an election... All local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election." National Academies Report, *supra* at 42, 80. In the Senate Intelligence Committee's recent report on election interference in the 2016 Presidential Election, the Committee said that "machines with electronic interfaces that electronically store votes (as opposed to paper ballots or optical scanners)—are used in

[17] https://doi.org/10.1109/MSECP.2004.1264852.

jurisdictions in 30 states and are at highest risk for security flaws […] [a]t a minimum, any machine purchased going forward should have a voter-verified paper trail." Senate Select Comm. On Intelligence, 115th Cong., Russian Targeting of Election Infrastructure During the 2016 Election (May 8, 2018).[18] Since the November 2016 election, ten states have improved or established auditing requirements. Nat'l Conference of State Legislatures, *Post-Election Audits* (Jan. 3, 2019).[19]

According to leading computer scientists, the inability to audit the results produced by DRE machines results in a chronic inability to identify errors, whether slight or egregious. As Ron Rivest has explained, "no meaningful audit of the DRE's electronic records to determine their accuracy is possible; accuracy can only be estimated by a variety of other (imperfect) measures, such as comparing the accumulated tallies to pre-election canvassing results, performing software code reviews, and testing the system accuracy before (or even during) the election." Rivest, *supra*, at 3760. Peter Neumann has stated, "[o]f course, all voting systems are subject to varying degrees of errors and manipulations; however, the unauditable all-electronic

[18] https://www.burr.senate.gov/imo/media/doc/One-Pager%20Recs%20FINAL%20VERSION%203-20.pdf.
[19] http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx

systems without voter-verified audit trials create a situation in which very small flaws or illicit software changes can result in widespread systematic alterations of the intended results." Hearing of the Calif. Assemb. Comm. on Reapportionment and Constitutional Amendments, 2003-04 Sess. (testimony of Peter G. Neumann, Principal Scientist, Computer Science Lab, SRI International).[20]

The failure to detect election interference does not mean that there is none; rather, the ongoing attacks reflect the ability of malicious actors to target the vulnerabilities of DRE machines. Danielle Root et al., *Election Security in All 50 States*, Center for American Progress (Feb. 12, 2018).[21]

In New Jersey, Florida, and North Carolina, paperless electronic voting systems caused the irrecoverable loss or miscount of votes in crucial elections. Greg Adomaitis, *Electronic Voting Case Prompts New Election, Investigation In Fairfield*, NJ.com (Sept. 1, 2011) (where the discrepancies based on DREs resulting in the voiding of an election, where the Superior Court judge said, "I have my suspicions that something that happened here was improper," but he did not "and may never" know, what exactly took place);[22] Douglas W.

---

[20] http://www.csl.sri.com/users/neumann/calvot04.pdf.
[21]https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.
[22] https://www.nj.com/cumberland/2011/09/touch-screen_voting_case_promp.html.

Jones & Barbara Simons, *Broken Ballots: Will Your Vote Count* (Center for the Study of Language and Information, 2012) (describing a 2006 Florida election in which almost 13% of voters did not select a candidate in the Congressional race, even though only 1.2% did not vote in the Senate contest, demonstrating a significant discrepancy, but paperless DREs prevented a recount).

Voter-verifiable paper ballots are essential for meaningful post-election audits, which are required in 34 states. *State Audit Laws National Database*, Verified Voting (2019).[23] In a secure election system, the EAC Guidelines recommends, "[t]he source and integrity of electronic tabulation reports are verifiable." EAC Guidelines, *supra* at Principle 13. The best practice currently available is to use hand-marked paper ballots. Andrew Appel, *Continuous-roll VVPAT under glass: an idea whose time has passed*, Freedom to Tinker (Oct. 19, 2018).[24] There are also ongoing efforts by technologists to develop better models for conducting more private, secure, and reliable balloting methods for public elections. *See* SSITH Secure Hardware Demo,

[23] https://www.verifiedvoting.org/state-audit-laws/.
[24] https://freedom-to-tinker.com/2018/10/19/continuous-roll-vvpat-under-glass-an-idea-whose-time-has-passed/.

Free & Fair (2019);[25] Anna Lysyanskaya et al., *Verifiable Elections That Scale for Free*, Public-Key Cryptography - PKC 2013 (Feb. 2013);[26] David Chaum, *Scantegrity* (2008);[27] Ronald L. Rivest & Warren D. Smith, *Three Voting Protocols: ThreeBallot, VAV, and Twin*, USENIX/ACCURATE Electronic Voting Technology Workshop (2007);[28] Tal Moran & Moni Naor, *Receipt-Free Universally-Verifiable Voting with Everlasting Privacy*, Advances in Cryptology - CRYPTO 2006 (Dwork C. eds., 2006).[29] The National Academies emphasizes the important role paper plays in election integrity:

> The ability of each voter to verify that a paper ballot correctly records his or her choices, before the ballot is cast, means that the collection of cast paper ballots forms a body of evidence that is not subject to manipulation by faulty hardware or software. These cast paper ballots may be recounted after the election or may be selectively examined by hand in a post-election audit. Such an evidence trail is generally preferred over electronic evidence like electronic cast-vote records or ballot images. Electronic evidence can be altered by compromised or faulty hardware or software. Paper ballots are designed to provide a human-readable recording of a voter's choices.

---

[25] https://freeandfair.us/ssith-secure-hardware-demo/.
[26] https://www.microsoft.com/en-us/research/publication/verifiable-elections-that-scale-for-free/.
[27] http://scantegrity.org.
[28] https://people.csail.mit.edu/rivest/RivestSmith-ThreeVotingProtocolsThreeBallotVAVAndTwin.pdf.
[29] https://link.springer.com/chapter/10.1007/11818175_22.

National Academies Report, *supra*, at 94.

Many DREs, but not those in Georgia, are equipped with a voter-verifiable paper audit trail (VVPAT) that prints voters' selections on paper and allows voters to confirm their selections by inspecting this paper prior to casting their vote. National Academies Report, *supra*, at 41. However, "[r]esearch suggests that DRE VVPATs tend not to be voter verified. This suggests that VVPATs may be of little value as a check on the accuracy of DREs." National Academies Report, *supra*, at 43. By comparison, hand-marked paper ballots fed into optical scanning machines allow for voter verification, cost less than electronic voting machines, and provide a paper trail for post-election audits.

II. Georgia's DRE voting systems fail to safeguard the secret ballot.

A. The secret ballot is the kernel of the American election system.

In the colonial era, elections were typically not secret; instead, most elected officials were elected by voice vote or a show of hands. *Burson v. Freeman*, 504 U.S. 191, 201 (1992) (citing E. Evans, A History of the Australian Ballot System in the United States (1917)). States gradually incorporated paper ballots into their elections, which voters crafted themselves. *Id.* (citing S. Albright, The American Ballot (1942)). Political

parties took advantage of the system by producing their own easily identifiable ballots for voters, creating a scheme of vote buying and selling fraught with intimidation and, often, violence. *Id*.

In 1888, the Louisville, KY municipal government adopted the first ballot law in the United States that provided for voting in secret by paper ballot. E. Evans, A History of the Australian Ballot System in the United States, 19 (1917). Only candidates who received their nomination by 50 or more voters were placed on the ballot, which was printed at the expense of the city. *Id*. Candidates' names were printed in alphabetical order, without party designations. *Id*. Later that year, Massachusetts and New York adopted a similar ballot system. *Id*. (citing Annals of the American Academy of Political and Social Sciences, pp. 735-36.) The system was a success and other states quickly followed, with 90 percent of the states adopting the Australian Ballot system by 1896.

One hundred twenty years later, the concept of the secret ballot remains a cornerstone of our democratic process. The U.S. Supreme Court recently noted the importance of this historical evolution in *Minn. Voters All. v. Mansky*, underscoring that universal political speech restrictions at polling places emerge from a respect for ballot secrecy:

> Between 1888 and 1896, nearly every State adopted the secret ballot. Because voters now needed to mark their state-printed ballots on-site and in secret, voting moved into a sequestered space where the voters could "deliberate and make a decision in . . . privacy."

Minn. Voters All. v. Mansky, 138 S. Ct. 1876, 1883 (2018).

In the 1992 case of *Burson v. Freeman*, the Supreme Court described voter privacy as a means of preventing voter fraud while protecting against undue coercion. Upholding a Tennessee statute that prohibited political candidates from campaigning within 100 feet of a polling place entrance, the Court stated:

> [A]n examination of the history of election regulation in this country reveals a persistent battle against two evils: voter intimidation and election fraud. After an unsuccessful experiment with an unofficial ballot system, all 50 States, together with numerous other Western democracies, settled on the same solution: a secret ballot secured in part by a restricted zone around the voting compartments. We find that this widespread and timetested consensus demonstrates that some restricted zone is necessary in order to serve the States' compelling interests in preventing voter intimidation and election fraud.

Burson, 504 U.S. at 206. In *McIntyre v. Ohio Elections Comm'n*, upholding the right to speak anonymously, the Supreme Court noted the close tie to the "hard-won right" to the secret ballot, writing:

> The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as

> possible… the Court's reasoning [in an earlier case] embraced a respected tradition of anonymity in the advocacy of political causes. This tradition is perhaps best exemplified by the secret ballot, the hard-won right to vote one's conscience without fear of retaliation.

McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341-43 (1995). In a brief for the U.S. Supreme Court, *amici* EPIC has previously explained that revealing the names of those who sign petitions would subject signatories to the risk of retribution, that signing petitions constitutes anonymous speech, and that signing petitions is similar to casting a vote and should be protected accordingly. Brief of *Amici Curiae* Electronic Privacy Information Center (EPIC) and Legal Scholars and Technical Experts in Support of the Petitioners, *Doe v. Reed*, 561 US 186 (2010) (No. 09-559).[30]

B. Georgia's DRE systems place at risk the identity of voters and the integrity of our elections.

Some DRE systems, including the ones in use in Georgia, place at risk the identity of voters and the integrity our elections. California's top-to-bottom review found that "the [Diebold AccuVote TSX] stores votes in the order in which they were cast; it stores them together with a record of the time they were cast and, if a specific configuration option is enabled, prints this time in a barcode on the paper VVPAT record; and it assigns them each

[30] https://epic.org/privacy/reed/EPIC_amicus_Reed.pdf.

an encrypted serial number that can be decrypted to discover the order of voting. Any one of these problems could leak enough information about the votes to reveal how individuals voted." Calandrino, *supra*, at 17. A spokesman for Diebold claimed that they don't timestamp ballots, even though the opposite has been proven true. Declan McCullagh, *E-voting predicament: Not-so-secret ballots*, CNET (Aug. 20, 2007).[31] Electronic voting machines by other vendors have been shown to have similar issues – both Hart and Sequoia's systems randomize ballots, but in way that can be easily reconstructed. Srinivas Inguva et al., *Source Code Review of the Hart InterCivic Voting System* 59, Univ. of Cal. (July 20, 2007);[32] Matt Blaze et al., *Source Code Review of the Sequoia Voting System*, Univ. of Cal. (July 20, 2007);[33] Edward Felten, *E-Voting Ballots Not Secret; Vendors Don't See Problem* (Aug. 20, 2007).[34]

[31] https://www.cnet.com/news/e-voting-predicament-not-so-secret-ballots/.
[32] https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/Hart-source-public.pdf.
[33] https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/sequoia-source-public-jul26.pdf.
[34] https://freedom-to-tinker.com/2007/08/20/e-voting-ballots-not-secret-vendors-dont-see-problem/.

C. The secret ballot safeguards privacy, freedom of association, and democratic values.

The secret ballot reduces the threat of coercion, vote buying and selling, and tampering. For individual voters, it provides the ability to exercise their right to vote without intimidation or retaliation. Ballot secrecy is a cornerstone of modern democracies. As the National Academy of Sciences recently found, "If anonymity is compromised, voters may not express their true preferences." National Academies Report, *supra* at 87. Because of the documented history of voter intimidation, coercion, and fraud associated with third-party knowledge of how individual voters cast their ballots, voter privacy remains central to election integrity. No community is immune to the effects of voter manipulation, but some communities are more vulnerable than others.

Federal and state courts, as well as legislatures, have historically taken steps to protect the right of voters to vote their conscience without fear of retaliation. A state survey conducted by EPIC, Common Cause, and Verified Voting in 2016 found that the vast majority of states (44) have constitutional provisions guaranteeing secrecy in voting, while the remaining states have statutory provisions referencing secrecy in voting. Caitriona Fitzgerald, Susannah Goodman, and Pamela Smith, *The Secret Ballot at Risk:*

Recommendations for Protecting Democracy (Aug. 2016).[35] The Supreme Court in its 1976 opinion in *Buckley v. Valeo*, stated that, "Secrecy, like privacy, is not per se criminal. On the contrary, secrecy and privacy as to political preferences and convictions are fundamental in a free society. For example, one of the great political reforms was the advent of the secret ballot as a universal practice." *Buckley v. Valeo*, 424 U.S. 1, 237 (1976).

The EAC Guidelines make clear that voting systems should protect the secrecy of voters' ballot selection:

> 10.1 - Ballot secrecy is maintained throughout the voting process.
> 10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

EAC Guidelines, Principle 10.

Ballot secrecy is so essential to the free exercise of the right to vote that the United States, by law, will not recognize foreign states as a democracy unless they provide for voting "by secret ballot." 22 U.S.C. § 8203(6)(B). (In determining whether a country is a democratic, the Secretary shall "conduct assessments of such conditions in countries and whether the country exhibits the following characteristics" including whether the "national legislative body

[35] https://secretballotatrisk.org.

of such country . . . are chosen by free, fair, open, and periodic elections, by universal and equal suffrage, and by secret ballot.")

The secret ballot is an integral requirement of democratic governance.

CONCLUSION

For the foregoing reasons, the Court should grant the Coalition Plaintiffs' motion for a preliminary injunction.

Dated: June 28, 2019

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

/s/ Alan Butler
Alan Butler (pro hac vice)
EPIC Senior Counsel

Caitriona Fitzgerald
EPIC Policy Director

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W. Suite 200
Washington, D.C. 20009
(202) 483-1140

s/ Russell T. Abney
Russell T. Abney (Ga. Bar No. 000875)
Ferrer Poirot Wansbrough
2100 RiverEdge Parkway Suite 1025
Atlanta, GA 30328
(800) 661-8210

Counsel for *Amici Curiae* Electronic Privacy Information Center